[h5] **What is Claimed is:**

[1 (c1)]
A portable keying device for installing a data communications encryption key in at least one electronic terminal, the electronic terminal including a secure encryption key memory location for storing at least one data communications encryption key, the device comprising:
a memory device for storing the at least one data communications encryption key; and
a communications unit coupled to the memory device, the communications unit being operative to transmit the at least one data communications encryption key in a predetermined format to the electronic terminal.

[2 (c2)]
The device of claim 1, wherein the communications unit includes a low power-close proximity RF transceiver.

[3 (c3)]
The device of claim 2, wherein the predetermined format includes transmitting an RF signal at a predetermined power level.

[4 (c4)]
The device of claim 3, wherein the predetermined power level is less than or equal to 1mW.

[5 (c5)]
The device of claim 3, wherein the RF signal has an effective range of less than or equal to a meter.

[6 (c6)]
The device of claim 2, wherein the predetermined format includes transmitting an RF signal in a predetermined direction.

[7 (c7)]
The device of claim 2, wherein the predetermined format includes transmitting an RF signal having a predetermined polarity.

[8 (c8)]
The device of claim 1, wherein the at least one data communications encryption key is installed in the electronic terminal in accordance with a predetermined protocol.

[9 (c9)]
The device of claim 8, wherein the predetermined protocol includes:
performing a handshaking routine, whereby the keying device and the electronic terminal exchange handshaking messages;
transmitting the at least one data communications encryption key from the keying device to

the electronic terminal in response to a successful handshaking routine;
validating the step of transmitting by re-transmitting the at least one data communications encryption key from the electronic terminal to the keying device, whereby the keying device compares the transmitted data communications encryption key to the re-transmitted data communications encryption key; and
storing the at least one data communications encryption key in the secure encryption key memory location in response to a successful step of validating.

[10 (c10)]
The device of claim 8, wherein the step of validating includes transmitting a test data communications encryption key from the keying device to the electronic terminal.

[11 (c11)]
The device of claim 10, wherein the electronic terminal compares the test data communications encryption key with a currently in-use data communications encryption key stored in the secure encryption key memory location.

[12 (c12)]
The device of claim 1, wherein the secure encryption key memory location is a memory location in non-volatile memory.

[13 (c13)]
The device of claim 12, wherein the non-volatile memory includes E^2PROM.

[14 (c14)]
The device of claim 12, wherein the non-volatile memory includes EPROM.

[15 (c15)]
The device of claim 12, wherein the non-volatile memory includes Flash memory.

[16 (c16)]
The device of claim 12, wherein the non-volatile memory includes battery-backed RAM.

[17 (c17)]
The device of claim 12, wherein the non-volatile memory includes Ferro RAM.

[18 (c18)]
The device of claim 1, wherein the communications unit includes an optical signaling unit.

[19 (c19)]
The device of claim 18, wherein the optical signaling unit is operative to transmit infrared radiation.

[20 (c20)]
The device of claim 1, wherein the communications unit includes an audio signaling unit.

[21 (c21)]
The device of claim 20, wherein the audio signaling unit communicates using DTMF signaling.

[22 (c22)]
The device of claim 1, further comprising an I/O device for receiving an encryption key from an external source.

[23 (c23)]
The device of claim 22, wherein the I/O device includes a keypad, the keypad being adapted to enter the at least one data communications encryption key.

[24 (c24)]
The device of claim 22, wherein the I/O device includes an external device interface adapted to receive the at least one data communications encryption key from an external device.

[25 (c25)]
The device of claim 1, further comprising:
an I/O device for receiving an initial encryption key from an external encryption key source; and
a processor coupled to the I/O device, the processor being programmed to generate the at least one data communications encryption key from the initial encryption key using a secure key generation algorithm.

[26 (c26)]
The device of claim 25, wherein the I/O device includes a keypad, the keypad being adapted to enter the initial encryption key.

[27 (c27)]
The device of claim 25, wherein the I/O device includes an external device interface adapted to receive the initial encryption key from an external device.

[28 (c28)]
A method for installing a data communications encryption key in an electronic terminal, the electronic terminal including a secure encryption key memory location for storing the at least one data communications encryption key, the method comprising:
providing a portable keying device, whereby the portable keying device is physically separated from the electronic terminal;
performing a handshaking routine, whereby the keying device and the electronic terminal exchange handshaking messages;
transmitting an encryption key from the portable keying device to the electronic terminal; and

storing the encryption key transmitted from the portable keying device to the electronic terminal in the secure key memory location.

[29 (c29)]
The method of claim 28, wherein the step of performing a handshaking routine includes transmitting an authorization signal from the portable keying device to the electronic terminal.

[30 (c30)]
The method of claim 29, wherein the portable keying device provides the electronic terminal with a predetermined authorization code during the step of transmitting an authorization signal.

[31 (c31)]
The method of claim 28, wherein the step of performing a handshaking routine includes transmitting RF signals having at least one predetermined transmission characteristic.

[32 (c32)]
The method of claim 31, wherein the at least one predetermined transmission characteristic includes transmitting an RF signal having a predetermined range.

[33 (c33)]
The method of claim 31, wherein the at least one predetermined transmission characteristic includes transmitting an RF signal in a predetermined direction.

[34 (c34)]
The method of claim 31, wherein the at least one predetermined transmission characteristic includes a transmitting an RF signal having a predetermined polarity.

[35 (c35)]
The method of claim 31, wherein the at least one predetermined transmission characteristic includes transmitting an RF signal having a predetermined modulation format that is characterized by a predetermined programming voltage.

[36 (c36)]
The method of claim 29, wherein the step of transmitting an encryption key further comprises:
transmitting the at least one data communications encryption key from the keying device to the electronic terminal in response to a successful handshaking routine;
validating the step of transmitting by re-transmitting the at least one data communications encryption key from the electronic terminal to the keying device, whereby the keying device compares the transmitted data communications encryption key to the re-transmitted data communications encryption key; and
storing the at least one data communications encryption key in the secure encryption key memory location in response to a successful step of validating.

[37 (c37)]
The method of claim 36, wherein the step of validating includes transmitting a test data communications encryption key from the keying device to the electronic terminal before transmitting the at least one data communications encryption key.

[38 (c38)]
The method of claim 37, wherein the step of validating includes the electronic terminal comparing the test data communications encryption key with a currently in-use data communications encryption key stored in the secure encryption key memory location.

[39 (c39)]
The method of claim 28, wherein the step of performing a handshaking routine includes transmitting infrared signals having at least one predetermined transmission characteristic.

[40 (c40)]
The method of claim 28, wherein the step of performing a handshaking routine includes transmitting audio signals having at least one predetermined transmission characteristic.

[41 (c41)]
The method of claim 40, wherein the audio signals include DTMF signals.

[42 (c42)]
A portable key installation system for installing a data communications encryption key, the system comprising:
at least one electronic terminal having a secure encryption key memory adapted to store the at least one data communications encryption key, and a terminal communications unit coupled to the secure encryption key memory; and
a portable keying device including a memory adapted to store the at least one data communications encryption key, and a device communications unit coupled to the memory device, the device communications unit being adapted to bi-directionally communicate the at least one data communications encryption key in a predetermined format to the terminal communications unit.

[43 (c43)]
The device of claim 42, wherein the terminal communications unit and the device communications unit include low power-close proximity RF transceivers.

[44 (c44)]
The device of claim 43, wherein the predetermined format includes transmitting an RF signal at a predetermined power level.

[45 (c45)]
The device of claim 44, wherein the predetermined power level is less than or equal to 1mW.

[46 (c46)]
The device of claim 44, wherein the RF signal has an effective range of less than or equal to a

meter.

[47 (c47)]
The device of claim 43, wherein the predetermined format includes transmitting an RF signal in a predetermined direction.

[48 (c48)]
The device of claim 43, wherein the predetermined format includes transmitting an RF signal having a predetermined polarity.

[49 (c49)]
The system of claim 43, wherein the at least one electronic terminal includes a programming voltage supply unit, the programming voltage supply unit being adapted to convert an RF signal transmitted by the device communications unit into programming voltage to thereby enable the secure encryption key memory to store the at least one data communications encryption key transmitted by the device communications unit.

[50 (c50)]
The system of claim 49, wherein the programming voltage supply unit comprises:
at least one capacitor coupled to the RF transceiver; and
a voltage regulator coupled to the at least one capacitor and the secure encryption key memory.

[51 (c51)]
The system of claim 50, wherein the at least one capacitor includes a plurality of capacitors.

[52 (c52)]
The system of claim 50, further comprising a diode disposed between the programming voltage supply unit and the RF transceiver.

[53 (c53)]
The system of claim 50, further comprising a battery coupled to the programming voltage supply unit.

[54 (c54)]
The system of claim 50, further comprising a normal voltage supply unit, the normal voltage supply unit including:
at least one second capacitor coupled to the RF transceiver; and
a second voltage regulator coupled to the at least one second capacitor and the secure encryption key memory.

[55 (c55)]
The system of claim 50, further comprising a switch disposed between the programming

voltage supply unit and the secure encryption key memory, the programming voltage being supplied to the secure encryption key memory when the switch is closed.

[56 (c56)]
The system of claim 43, further comprising:
a battery coupled to the RF transceiver of the electronic terminal;
at least one capacitor coupled to the battery, the at least one capacitor being charged by the battery to generate a programming voltage, whereby the secure encryption key memory is enabled to store the at least one data communications encryption key transmitted by the device communications unit; and
a voltage regulator coupled to the at least one capacitor.

[57 (c57)]
The system of claim 56, further comprising a switch disposed between the at least one capacitor and the secure encryption key memory, the programming voltage being supplied to the secure encryption key memory when the switch is closed.